80655

C 56 37

IDEP FORM NO. 17-10-62 IDEP

GENERAL REPORT SUMMARY SHEET

1. COMPONENT PART NAME PER GENERIC CODE General Technical Data - Parts Test of Reliability Mathematics	2. PROGRAM OR WEAPON SYSTEM APOLLO	3. DAY MO. YR. TEST COMPL. REPT. COMPL. 15 6 66
	5. ORIGINATOR'S REPORT NO. SID-66-744 (14)	
4. ORIGINATOR'S REPORT TITLE (6) CALCULATIONS OF RELIABILITY PREDICTIONS FOR THE APOLLO SPACECRAFT	6. TEST TYPE, ETC. Systems Predictions	

7. THIS TEST (SUPERSEDES) (SUPPLEMENTS) REPORT NO:

8. OUTLINE, TABLE OF CONTENTS, SUMMARY, OR EQUIVALENT DESCRIPTION:

(10) B. L. Amstadter
Bertram

(11) 15 Jun 66

(12) 71 p.

(15) NAS 9-150

ABSTRACT

This document defines a new method of reliability prediction for complex systems. The method involves calculation of both upper and lower bounds, and a procedure for combining the two to yield an approximately true prediction value. Both mission success and crew safety predictions can be calculated, and success probabilities can be obtained for individual mission phases or subsystems. Primary consideration is given to evaluating cases involving zero or one failure per subsystem, and the results of these evaluations are then used for analyzing multiple failure cases. Extensive development is provided for the overall mission success and crew safety equations for both the upper and lower bounds. Sufficient explanation of individual phase and subsystem equations is given so that their deviations can be determined easily by the reader.

Following the main body of the report, a short appendix is provided which delineates the specific data required from the reliability analysts. The objective of the method was to simplify the data requirements as much as possible, and to include the resulting complexity in the prediction method itself.

A computer program was developed to perform the calculations indicated by the equations. To optimize computer utilization, the program deviates from the text with respect to the sequence of the mathematical operations. An explanation of the program is a second appendix to this report. A sample of the computer output is a third appendix.

(18) IDEP

DDC RECEIVED FEB 8 1967

RECEIVED 23 SEP 1966

11. REPT NO 347.40.00.00-F1-47

9. SIGNED C.F. Kirkpatrick	10. CONTRACTOR NAA-S&ID	SUBCONTRACTOR

REPRODUCTION OR DISPLAY OF THIS MATERIAL FOR SALES OR PUBLICITY PURPOSES IS PROHIBITED

NOTICES PAGE

Foreign Nation Release

This information is furnished upon the condition that it will not be released to another Nation without specific authority of the cognizant agency (Military or NASA) of the United States Government, and that the information be provided substantially the same degree of protection afforded it by the Department of Defense of the United States.

Disclaimer of Liability from Act of Transmittal

When Government drawings, specifications, or other data are used for any purpose other than in connection with a definitely related Government procurement operation, the United States Government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specification, or other data, is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying and rights or permission to manufacture, use, or sell any patented invention that may in any be related thereto.

Any information disseminated by the Data Distribution Centers of the Interagency Data Exchange Program is intended to promote test data utilization in the National interest among groups engaged in Ballistic Missile, Space Vehicle and related programs.

Dissemination of said information does not imply verification or endorsement of the information. The originator, in submitting the material is acting in accordance with the requirements of his contract, and neither the originator nor the disseminator assumes any liability to parties adopting any product, process or practice based upon the usage of the information. Its presenting the success or failure of one (or several) part number(s), model(s), lot(s) under specific environment and output requirements, does not imply that other products not herein reported on are either inferior or superior.

Omission of Charges for Follow-on Actions

Any compliance by the report originator with requests from recipients for more detailed information on IDEP reports originated under Government contracts will be considered within the scope of present contractual obligations. Compliance with such requests will be at the discretion of the report originator and will be performed without cost or obligation to the requestor unless otherwise negotiated in advance.

Reproduction of this Report

Reproduction or duplication of any portion of this report is expressly forbidden, except by those contractors receiving it directly from the Data Centers or originator, for their internal use or the use of their sub-contractors. Reproduction or display of all or any portion of this material for any sales, advertising of publicity purposes is prohibited.

ACCESSION for

CFSTI WHITE SECTION ☐

DDC BUFF SECTION ☑

UNANNOUNCED ☐

JUSTIFICATION ....

....

BY fm ....

DISTRIBUTION/AVAILABILITY CODES

DIST.	AVAIL. and/or SPECIAL	
3		

Each transmittal of this document outside the agencies of the U. S. Government must have prior approval of:

Hq Space Systems Division
Attn: IDEP Office (SSSD)
Air Force Unit Post Office
Los Angeles, California 90045

The above limitation does not apply to IDEP participants.

SID 66-744

CALCULATIONS OF RELIABILITY PREDICTIONS FOR THE APOLLO SPACECRAFT

NAS9-150

15 June 1966

Prepared by

B.L. Amstadter

Approved by

C. O. Baker, Manager
Apollo Reliability

NORTH AMERICAN AVIATION, INC.
SPACE and INFORMATION SYSTEMS DIVISION

TECHNICAL REPORT INDEX/ABSTRACT

ACCESSION NUMBER	DOCUMENT SECURITY CLASSIFICATION UNCLASSIFIED
TITLE OF DOCUMENT CALCULATIONS OF RELIABILITY PREDICTIONS FOR THE APOLLO SPACECRAFT	LIBRARY USE ONLY
AUTHOR(S) AMSTADTER, BERTRAM L.	

CODE	ORIGINATING AGENCY AND OTHER SOURCES	DOCUMENT NUMBER
NAJ65231	SPACE AND INFORMATION SYSTEMS DIV. OF NAA, DOWNEY, CALIF.	SID 66-744

PUBLICATION DATE	CONTRACT NUMBER
15JUN66	NAS9-150

DESCRIPTIVE TERMS

RELIABILITY PREDICTIONS
APOLLO
SUBSYSTEM RELIABILITY
CREW SAFETY

ABSTRACT

THIS DOCUMENT DEFINES A NEW METHOD OF RELIABILITY PREDICTION FOR COMPLEX SYSTEMS. THE METHOD INVOLVES CALCULATION OF BOTH UPPER AND LOWER BOUNDS, AND A PROCEDURE FOR COMBINING THE TWO TO YIELD AN APPROXIMATELY TRUE PREDICTION VALUE. BOTH MISSION SUCCESS AND CREW SAFETY PREDICTIONS CAN BE CALCULATED, AND SUCCESS PROBABILITIES CAN BE OBTAINED FOR INDIVIDUAL MISSION PHASES OR SUBSYSTEMS. PRIMARY CONSIDERATION IS GIVEN TO EVALUATING CASES INVOLVING ZERO OR ONE FAILURE PER SUBSYSTEM, AND THE RESULTS OF THESE EVALUATIONS ARE THEN USED FOR ANALYZING MULTIPLE FAILURE CASES. EXTENSIVE DEVELOPMENT IS PROVIDED FOR THE OVERALL MISSION SUCCESS AND CREW SAFETY EQUATIONS FOR BOTH THE UPPER AND LOWER BOUNDS. SUFFICIENT EXPLANATION OF INDIVIDUAL PHASE AND SUBSYSTEM EQUATIONS IS GIVEN SO THAT THEIR DEVIATIONS CAN BE DETERMINED EASILY BY THE READER.

FOLLOWING THE MAIN BODY OF THE REPORT, A SHORT APPENDIX IS PROVIDED WHICH DELINEATES THE SPECIFIC DATA REQUIRED FROM THE RELIABILITY ANALYSTS. THE OBJECTIVE OF THE METHOD WAS TO SIMPLIFY THE DATA REQUIREMENTS AS MUCH AS POSSIBLE, AND TO INCLUDE THE RESULTING COMPLEXITY IN THE PREDICTION METHOD ITSELF.

A COMPUTER PROGRAM WAS DEVELOPED TO PERFORM THE CALCULATIONS INDICATED BY THE EQUATIONS. TO OPTIMIZE COMPUTER UTILIZATION, THE PROGRAM DEVIATES FROM THE TEXT WITH RESPECT TO THE SEQUENCE OF THE MATHEMATICAL OPERATIONS. AN EXPLANATION OF THE PROGRAM IS A SECOND APPENDIX TO THIS REPORT. A SAMPLE OF THE COMPUTER OUTPUT IS A THIRD APPENDIX.

CONTENTS

BLANK PAGE

RELIABILITY PREDICTION METHODS FOR THE APOLLO SPACECRAFT

SUMMARY

The complexity of the Apollo Spacecraft and missions has necessitated a reevaluation of methods for prediction of reliability. It has been found that exact analytical methods are either difficult to define or so detailed or complex that they cannot readily be used. Some degree of success in performing predictions has been achieved through the use of simulation models (Monte Carlo techniques). However, these have proved excessively expensive, particularly when very high overall reliabilities are involved. This is because the degree of accuracy is dependent on the number of simulation trials, and a greater number of trials is required for the same degree of accuracy for high reliabilities than for lower reliabilities.

As a result of these limitations, attempts have been made to calculate reliability prediction numerics by using approximate analytical methods. Some of these approximate methods involve calculation of only a lower bound, and provide sufficient proof that the true prediction number is higher than the calculated number. How much higher, however, has been difficult to determine, even approximately. The original method used by S&ID overcame this difficulty by calculating both an upper and a lower bound and, by an empirical method, computing an approximately true value. The upper bound was found by subtracting failure cases from unity, while the lower bound was found by adding success cases. All calculations were performed using desk calculators and manual methods, with the resulting limitation that only simple success and failure cases could be considered. This led to considerable differential between the two bounds. An important advantage, however, was the ability to detect inconsistencies and anomalies in the input data and secure rapid correction.

Since development of the previous approximate analytical method, further expansion of the techniques has been made so that all cases can be considered. This was made possible through thorough evaluation of both the original input and output numerics and determination of error magnitudes that could result from the approximations necessary for considering cases involving multiple failures. More exact calculations are used for zero and one-failure cases, resulting in consideration of a higher percentage of the total number of cases. The number of multiple-failure cases is thereby reduced to a level where the simplifications used would not significantly affect the overall results. The modifications, greater exactness, and expanded number of cases led to utilization of a computer program to perform the numerical operations, while still permitting visual (manual)

evaluation of input data. The current methods apply to calculation of crew safety probability and also provide for determination of mission and crew loss probabilities by individual subsystem or phase. The computer performs essentially the same calculations described here, although the order is sometimes varied to facilitate optimum computer utilization.

MISSION SUCCESS - UPPER BOUND

The upper bound of the reliability prediction range for mission success is found by considering failures and, in effect, subtracting these from unity. Only series elements in the mission continuation logic diagrams are considered. Mission success occurs when no series element fails in any subsystem in any phase of the mission — that is, the probability of mission success is the product of the reliabilities of all series elements. Element reliabilities are first combined into subsystem reliabilities from which the mission success probability is calculated.

$$R_{MS} = \prod_{\substack{i=1 \\ j=1}}^{\substack{j=m \\ i=n}} R_{i,j}$$

where

R_{MS} is the probability of mission success;

$R_{i,j}$ is the reliability of subsystem i in phase j;

m is the number of phases; and

n is the number of subsystems

An exponential model (constant failure-rate system) is assumed except for single-shot components. This approach is realistic because components are pretested and then operated within their normal useful life. It also facilitates calculations by making possible the suitable combination of reliabilities of various components. The exponential model is also used in all other predictions discussed in this report.

Since $R_{i,j} = e^{-F_{i,j}}$ where $F_{i,j}$ is the failure probability of subsystem i in phase j,

$$\prod_{\substack{i=1\\j=1}}^{\substack{m\\n}} R_{i,j} = e^{-F_{1,1}} \times e^{-F_{2,1}} \times \ldots e^{-F_{n,1}} \times e^{-F_{1,2}} \times \ldots e^{-F_{n,2}} \times \ldots e^{-F_{n,m}}$$

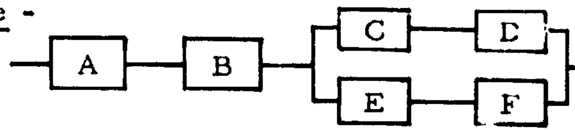
$$= e^{-(F_{1,1} + F_{2,1} + \ldots F_{n,1} + F_{1,2} + \ldots F_{n,2} + \ldots F_{n,m})}$$

$$\text{or} \quad R_{MS} = e^{-\sum_{\substack{i=1\\j=1}}^{\substack{m\\n}} F_{i,j}} \tag{1}$$

MISSION SUCCESS - LOWER BOUND

The lower bound for probability of mission success is found by adding success cases. It can be easily shown that for Apollo mission phases, when three or more possible paths exist, the resultant failure probability of the redundant components is less than 1×10^{-6} in all cases of current configurations. Therefore failure probabilities of components in such parallel paths are not included in the computation. All other components are included.

The success cases considered are those in which no failure occurs in any included component and those in which not more than one non-series component fails. Assuming the following simple logic diagram for one subsystem in one phase -



the probability of mission success is found by adding the probability of no failure of any component (A through F) to the sum of the probabilities of a failure of any one non-series component (C through F), the other components not failing.

$$R_{i,j} = (R_A \times R_B \times R_C \times R_D \times R_E \times R_F)$$
$$+ (R_A \times R_B \times Q_C \times R_D \times R_E \times R_F)$$
$$+ (R_A \times R_B \times R_C \times Q_D \times R_E \times R_F)$$
$$+ (R_A \times R_B \times R_C \times R_D \times Q_E \times R_F)$$
$$+ (R_A \times R_B \times R_C \times R_D \times R_E \times Q_F)$$

$$R_{i,j} = (R_A \times R_B \times R_C \times R_D \times R_E \times R_F)$$
$$+ \left(R_A \times R_B \times Q_C \times R_D \times R_E \times R_F \times \frac{R_C}{R_C}\right)$$
$$+ \left(R_A \times R_B \times R_C \times Q_D \times R_E \times R_F \times \frac{R_D}{R_D}\right)$$
$$+ \left(R_A \times R_B \times R_C \times R_D \times Q_E \times R_F \times \frac{R_E}{R_E}\right)$$
$$+ \left(R_A \times R_B \times R_C \times R_D \times R_E \times Q_F \times \frac{R_F}{R_F}\right)$$
$$= (R_A \times R_B \times R_C \times R_D \times R_E \times R_F)$$
$$+ (R_A \times R_B \times R_C \times R_D \times R_E \times R_F) \times \left(\frac{Q_C}{R_C} + \frac{Q_D}{R_D} + \frac{Q_E}{R_E} + \frac{Q_F}{R_F}\right)$$
$$= \prod_{k=A}^{F} R_{k_{i,j}} + \prod_{k=A}^{F} R_{k_{i,j}} \left(\Sigma \frac{Q_{k_{i,j}}}{R_{k_{i,j}}}\right)$$
$$= \prod_{k=A}^{F} R_{k_{i,j}} \left(1 + \Sigma \frac{Q_{k_{i,j}}}{R_{k_{i,j}}}\right)$$

where

$R_{k_{i,j}}$ is the reliability of component k of subsystem i in phase j;

$Q_{\dot{k}_{i,j}}$ is the probability of failure of a non-series component of subsystem i in phase j; and

$R_{\dot{k}_{i,j}}$ is the reliability of the non-series component.

Since $R_{k_{i,j}} = e^{-Q_{k_{i,j}}}$ where $Q_{k_{i,j}}$ is the probability of failure of any included component in subsystem i in phase j;

$$R_{i,j} = e^{-\Sigma Q_{k_{i,j}}} \left(1 + \Sigma \frac{Q_{\dot{k}_{i,j}}}{R_{\dot{k}_{i,j}}} \right)$$

However, $R_{\dot{k}_{i,j}}$ is frequently very close to unity for any one phase, and may then be omitted from the calculations giving the result:

$$\underline{R_{i,j} = e^{-\Sigma Q_{k_{i,j}}} \left(1 + \Sigma \dot{Q}_{k_{i,j}} \right)} \qquad (2)$$

Equation 2 is referenced later in this report, and its derivation is important to the analyses. When $R_{\dot{k}}$ is greater than 0.999, as is almost always true, Equation 2 is exact. The equation facilitates the rapid summation of individual component failure probabilities with minimum calculating time. (When $R_{\dot{k}}$ is less than 0.999, it is used in the calculation of Equation 2. Equation 2, as shown, will be used in this report, remembering that $R_{\dot{k}}$ is considered in the calculations, when appropriate.)

The subsystem-phase reliabilities are combined to obtain the overall mission success probability. Only one non-series failure per subsystem is considered, although any number of subsystems may have a failed component. The following notations are used for simplification:

$$F_{i,j} = \Sigma Q_{k_{i,j}} \quad \text{and} \quad \dot{F}_{i,j} = \Sigma Q_{\dot{k}_{i,j}}$$

Equation 2 thus becomes:

$$\underline{R_{i,j} = e^{-F_{i,j}}(1 + \dot{F}_{i,j})} \qquad (3)$$

The probability of no failures in subsystem i in phase j is:

$$\underline{e^{-F_{i,j}}} \qquad (4)$$

and the probability of exactly one non-series failure is:

$$\underline{e^{-F_{i,j}} \times \dot{F}_{i,j}} \qquad (5)$$

NOTE: In the lower bound case calculations, F includes both series and parallel components.

Since only one failure per subsystem is considered in the mission, the reliability of a subsystem is calculated by summing the probability of zero failures and all cases of the probability of one non-series failure.

$$\begin{aligned}
R_i = {} & e^{-F_{i,1}} \times e^{-F_{i,2}} \times e^{-F_{i,3}} \times \ldots\ldots e^{-F_{i,m}} \\
& + \left(e^{-F_{i,1}} \times \dot{F}_{i,1}\right) \times e^{-F_{i,2}} \times e^{-F_{i,3}} \times \ldots e^{-F_{i,m}} \\
& + e^{-F_{i,1}} \times \left(e^{-F_{i,2}} \times \dot{F}_{i,2}\right) \times e^{-F_{i,3}} \times \ldots e^{-F_{i,m}} \\
& \quad \vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots \\
& + e^{-F_{i,1}} \times e^{-F_{i,2}} \times e^{-F_{i,3}} \times \ldots \left(e^{-F_{i,m}} \times \dot{F}_{i,m}\right) \\
= {} & \left(e^{-F_{i,1}} \times e^{-F_{i,2}} \times e^{-F_{i,3}} \times \ldots\ldots e^{-F_{i,m}}\right) \\
& + \left(e^{-F_{i,1}} \times e^{-F_{i,2}} \times e^{-F_{i,3}} \times \ldots\ldots e^{-F_{i,m}}\right) \times (\dot{F}_{i,1} + \dot{F}_{i,2} + \dot{F}_{i,3} + \ldots \dot{F}_{i,m})
\end{aligned}$$

$$R_i = e^{-(F_{i,1}+F_{i,2}+F_{i,3}+\ldots F_{i,m})}$$

$$+ e^{-(F_{i,1}+F_{i,2}+F_{i,3}+\ldots F_{i,m})} \times (\dot{F}_{i,1} + \dot{F}_{i,2} + \dot{F}_{i,3} + \ldots \dot{F}_{i,m})$$

$$= e^{-\sum_{j=1}^{m} F_{i,j}} + e^{-\sum_{j=1}^{m} F_{i,j}} \left(\sum_{j=1}^{m} \dot{F}_{i,j}\right) = \underline{e^{-\sum_{j=1}^{m} F_{i,j}} \left(1 + \sum_{j=1}^{m} \dot{F}_{i,j}\right)} \tag{6}$$

NOTE: To simplify calculations, the original phase logic diagram associated with each phase is retained although it is recognized that a failure of a non-series element in one phase slightly modifies the logic diagrams for succeeding phases. This aoproach is conservative because acıually fewer components need be considered in phases subsequent to the failure.

The reliability of the system is the product of the reliabilities of all individual subsystems (from Equation 6):

$$R_{MS} = \prod_{i=1}^{n} R_i = \prod_{i=1}^{n} \left[e^{-\sum_{j=1}^{m} F_{i,j}} \left(1 + \sum_{j=1}^{m} \dot{F}_{i,j}\right)\right] = \prod_{i=1}^{n} \left(e^{-\sum_{j=1}^{m} F_{i,j}}\right) \times \prod_{i=1}^{n} \left(1 + \sum_{j=1}^{m} \dot{F}_{i,j}\right)$$

$$= \left(e^{-\sum_{j=1}^{m} F_{1,j}} \times e^{-\sum_{j=1}^{m} F_{2,j}} \times \ldots e^{-\sum_{j=1}^{m} F_{n,j}}\right) \times \prod_{i=1}^{n} \left(1 + \sum_{j=1}^{m} \dot{F}_{i,j}\right)$$

$$= \underline{e^{-\sum_{i=1}^{n} \sum_{j=1}^{m} F_{i,j}} \times \prod_{i=1}^{n} \left(1 + \sum_{j=1}^{m} \dot{F}_{i,j}\right)} \tag{7}$$

A small increment of mission success, ΔR_{MS}, is added to Equation 7. This is obtained from Equation 35.

It has been found empirically that an approximately true value of the failure probability can be obtained by taking the square root of the product of the upper and lower values of the probability of failure. From this, it follows that

$$R_{MS} = 1 - \sqrt{\left(1 - R_{MS}\right)_{upper} \times \left(1 - R_{MS}\right)_{lower}}$$

$$= 1 - \sqrt{\left(1 - e^{-\sum_{i=1}^{n}\sum_{j=1}^{m} F_{i,j}}\right)\left\{1 - \left[e^{-\sum_{i=1}^{n}\sum_{j=1}^{m} F_{i,j}} \times \prod_{i=1}^{n}\left(1 + \sum_{j=1}^{m} F_{i,j}\right) + \Delta R_{MS}\right]\right\}} \tag{8}$$

(from Eq. 1) (from Eq. 7) (from Eq. 35)

NOTE: F in $R_{MS_{upper}}$ considers only series components;

F in $R_{MS_{lower}}$ considers both series and parallel components.

CREW SAFETY - UPPER BOUND

The upper bound for crew safety is the sum of the probabilities of mission success (MS) and all possible safe aborts (SA) resulting from the failure of a series component.

$$R_{CS} = R_{MS} + R_{SA} \tag{9}$$

As in the case of the mission success upper bound, it is actually found by considering failures and the probabilities of their not occurring.

The probability of a safe abort is the product of the probability that an abort is required times the probability that it is successful. As a very close approximation, an abort is considered to take place at an average time of half way through the phase in which it is necessitated. (The greater the number of phases and the shorter each phase, the closer the approximation.)

Each abort case is calculated as a mutually exclusive event, thereby permitting the simple addition of all abort cases considered. An abort case is computed by taking the product of the following terms:

a. The probability of mission continuation (MC) for all subsystems up to the phase in which the abort occurs, (no series failures).

b. The probability that all subsystems except the one that failed perform satisfactorily for an average time of one-half of the phase in which an abort is required.

c. The probability that, in the phase, the subsystem under consideration incurs a failure that requires but does not preclude an abort—i.e., failure of a component that is in series in the MC logic diagram but is not in series in the SA logic diagram.

d. The probability that all subsystems except the one that failed perform satisfactorily during the abort—i.e., no failure of a series component in the normal abort logic diagram.

e. The probability that the failed subsystem performs satisfactorily during the abort—that is, incurs no failure of a series element in the modified abort logic diagram. The series elements in the modified diagram include the original series components plus the average number of additional components which become series elements as a result of the failure which occurred in the mission.

The terms a through e are found as follows:

a. Reliability of all subsystems up to phase of abort

$$= \prod_{\substack{i=1 \\ j=1}}^{\substack{n \\ \text{phase}-1}} R_{i,j} = e^{-\sum_{\substack{i=1 \\ j=1}}^{\substack{n \\ \text{phase}-1}} F_{i,j}} \qquad (10)$$

Derivation of this equation is the same as that for Equation 1.

b. Probability that all other subsystems perform for one-half of abort phase

$$= \prod_{\substack{i=1\\ j=\text{phase}-1}}^{\substack{\text{phase}-\frac{1}{2}\\ n-1}} R_{i,j} = \frac{\prod_{\substack{i=1\\ j=\text{phase}-1}}^{\substack{\text{phase}-\frac{1}{2}\\ n}} R_{i,j}}{\underset{j=\text{phase}-1}{\overset{\text{phase}-\frac{1}{2}}{R_{n,j}}}}$$

$$= \frac{e^{-\frac{1}{2}\sum_{i=1}^{n} F_{i,j}}\Big|_{j=\text{abort phase}}}{e^{-\frac{1}{2}F_{n,j}}} = \underline{e^{-\frac{1}{2}\sum_{i=1}^{n} F_{i,j}}\Big|_{j=\text{abort phase}} \times e^{+\frac{1}{2}F_{n,j}}} \tag{11}$$

c. Probability that subsystem n fails in phase j

$$= R_{n,j} \times F'_{n,j} = \underline{e^{-\frac{1}{2}F_{n,j}} \times F'_{n,j}\Big|_{j=\text{abort phase}}} \tag{12}$$

Derivation of this equation is similar to that for Equations 2 and 5, except that F'_n represents failures of subsystem n that require but do not preclude an abort, and the average time of abort is half way through the phase.

d. Probability that all other subsystems perform satisfactorily in abort

$$= \prod_{i=1}^{n-1} R_{i,j,\text{abort}} = \frac{\prod_{i=1}^{n} R_{i,j,\text{abort}}}{R_{n,j,\text{abort}}}$$

$$= \frac{e^{-\sum_{i=1}^{n} G_{i,j}}}{e^{-G_{n,j}}} = \frac{e^{-\sum_{i=1}^{n} G_{i,j}} \times e^{+G_{n,j}}}{} \tag{13}$$

where $G_{i,j}$ is the failure probability of subsystem i in abort in phase j.

e. Probability that subsystem n performs satisfactorily in abort = $R'_{n,j,\text{abort}} = e^{-G'_{n,j}}$ where $G'_{n,j}$ is the modified failure probability of subsystem n, $(=G_{n,j} + \Delta G_{n,j})$. Therefore,

$$R'_{n,j,\text{abort}} = e^{-(G_{n,j} + \Delta G_{n,j})} \tag{14}$$

Equations 10 through 14 are multiplied together to obtain the probability of safe abort of one subsystem in one phase.

$$R_{SA_{n,j}} = \left(e^{-\sum_{j=1}^{\text{phase}-1} \sum_{i=1}^{n} F_{i,j}} \right) \times \left(e^{-\frac{1}{2}\sum_{i=1}^{n} F_{i,j}} \times e^{+\frac{1}{2}F_{n,j}} \right)_{j=\text{abort phase}} \times \left(e^{-\frac{1}{2}F_{n,j}} \times F'_{n,j} \right)_{j=\text{abort phase}}$$

$$\times \left(e^{-\sum_{i=1}^{n} G_{i,j}} \times e^{+G_{n,j}} \right) \times \left(e^{-(G_{nj} + \Delta G_{n,j})} \right)$$

$$= \frac{e^{-\sum_{j=1}^{\text{phase}-1} \sum_{i=1}^{n} F_{i,j}} \times e^{-\frac{1}{2}\sum_{i=1}^{n} F_{i,j}} \times F'_{n,j} \times e^{-\sum_{i=1}^{n} G_{i,j}} \times e^{-\Delta G_{n,j}}}{} \tag{15}$$

When the abort is caused by failure of the Service Propulsion System (SPS) in the mission, another abort method may be used, depending on the mission. This may result in a changed abort logic diagram for the Service Module Reaction Control System (S/M RCS) and, in some cases, for other subsystems. A new probability of failure in abort, $GG_{i,j}$, is substituted for $G_{i,j}$ for the affected subsystems, where applicable, thus modifying Equations 13 and 15. This is done before summing $R_{SA_{i,j}}$.

The total number of safe aborts is the sum of the $R_{SA_{i,j}}$ terms:

$$R_{SA} = \sum_{\substack{i=1 \\ j=1}}^{\substack{m \\ n}} R_{SA_{i,j}} \quad \text{(from Equation 15 or modified 15)} \tag{16}$$

The overall upper bound for crew safety is the sum of Equations 1 and 16:

$$R_{CS_{upper}} = R_{MS_{upper}} + R_{SA_{upper}} \tag{9}$$

CREW SAFETY—LOWER BOUND

The most complex case is the lower-bound prediction of crew safety. The major reason for this complexity is the inability to account analytically for cases of multiple failures. Although analytical models and computer programs have been developed to evaluate multiple failures occurring in one phase, the failure probabilities cannot be evaluated when they occur in different phases, which is many times more likely. Consequently, an analytical method has been developed which provides a very close approximation to the true answer, and which can be shown to be on the conservative side, thereby providing a lower bound.

The lower bound for crew safety is found by adding the probability of mission success, all cases of the probability of safe abort with no more than one failure per subsystem in the mission and in the abort, and all other cases of safe abort. The first two of these probabilities are computed directly; the third utilizes a method of differences discussed in succeeding paragraphs.

The probability of mission success is obtained from Equation 7. The probability of safe abort with no more than one failure per subsystem is calculated as the product of several probabilities. However, there is more complexity in these calculations than for the upper bound because, for the lower bound, both series and parallel components are considered, and each subsystem may have one nonseries failure in either MC or SA or both. (The system which necessitated the abort has a noncatastrophic series failure in MC.) The failure permitted during abort depends on the condition of the system when the abort is started.

The probability of zero or one failure up to the time of abort is calculated from a modification of Equation 7. Equation 7 defines the reliability for all subsystems for all phases. This is modified by summing the number of phases from phase one to half-way through the phase in which the abort occurs, (phase - 1/2). The sum of failure probabilities from phase one through (phase - 1/2) can more easily be expressed as the sum from phase one through (phase -1) plus one-half the failure probability for the phase:

$$\sum_{j=1}^{j=\text{abort phase}-\frac{1}{2}} F_{i,j} = \sum_{j=1}^{\text{phase}-1} F_{i,j} + \tfrac{1}{2} F_{i,j}\Big|_{j=\text{abort phase}}$$

Since the abort is caused by the failure of a series component in one subsystem, the changed equation is further modified by dividing by the reliability of the subsystem which failed reference Equation 11. The resulting expression is:

$$\frac{e^{-\sum_{i=1}^{n}\left(\sum_{j=1}^{\text{phase}-1} F_{i,j} + \frac{1}{2} F_{i,j}\Big|_{j=\text{abort phase}}\right)} \times \prod_{i=1}^{n}\left(1 + \sum_{j=1}^{\text{phase}-1} \dot{F}_{i,j} + \frac{1}{2}\dot{F}_{i,j}\Big|_{j=\text{abort phase}}\right)}{e^{-\left(\sum_{j=1}^{\text{phase}-1} F_{n,j} + \frac{1}{2} F_{n,j}\Big|_{j=\text{abort phase}}\right)} \times \left(1 + \sum_{j=1}^{\text{phase}-1} \dot{F}_{n,j} + \frac{1}{2}\dot{F}_{n,j}\Big|_{j=\text{abort phase}}\right)} \tag{17}$$

Subsystem n, which incurred a noncatastrophic series failure in the mission, had no failure up to the abort phase and no other failure in the phase. From Equations 10 (modified) and 12, this probability is expressed as:

$$e^{-\sum_{j=1}^{\text{phase}-1} F_{n,j}} \times \left(e^{-\frac{1}{2} F_{n,j}} \times F'_{n,j}\right)_{j=\text{abort phase}} \tag{18}$$

In this set of cases, each subsystem except the one which had the series failure can achieve a successful abort if not more than one nonseries failure occurs in the abort. (A nonseries failure in MC does not generally affect the abort because a parallel element in MC is at least triply redundant in the abort logic.) Therefore, the probability of success of these subsystems in abort is expressed by:

$$e^{-\sum_{\substack{i=1 \\ j=\text{abort phase}}}^{n-1} G_{i,j}} \times \prod_{i=1}^{n-1} (1 + \dot{G}_{i,j}) = \frac{e^{-\sum_{i=1}^{n} G_{i,j}} \prod_{i=1}^{n} (1 + \dot{G}_{i,j})}{e^{-G_{n,j}} \times (1 + \dot{G}_{n,j})} \tag{19}$$

where

$G_{i,j}$ is the failure probability in abort in phase j of any included component of subsystem i (series or dual-parallel components);

$\dot{G}_{i,j}$ is the failure probability in abort in phase j of a non-series component of subsystem i;

$G_{n,j}$ is the failure probability in the abort of an included component of subsystem n which failed in the mission;

$\dot{G}_{n,j}$ is the failure probability in the abort of a non-series component of subsystem n.

Subsystem n, which had a noncatastrophic failure in the mission, has a modified abort logic. This includes the original components less one or more parallel components no longer applicable due to the mission failure. The probability of a successful abort is the sum of the probabilities of no failure, $e^{-G_{n,j}}$, and of not more than one non-series failure ($e^{-G'_{n,j}} \times \dot{G}'_{n,j}$). $G'_{n,j}$ is equal to $G_{n,j} - \Delta G_{n,j}$ where $-\Delta G_{n,j}$ accounts for the reduced probability. $\dot{G}'_{n,j}$ is equal to $\dot{G}_{n,j} - 2\Delta G_{n,j}$ because not only are one or more components no longer applicable, but their counterparts are no longer in parallel. Thus, the probability of subsystem n successfully completing the abort is:

$$\underline{e^{-(G_{n,j} - \Delta G_{n,j})} \times (1 + \dot{G}_{n,j} - 2\Delta G_{n,j})} \tag{20}$$

The probability of safe abort for the cases of not more than one failure per subsystem in the mission, for one subsystem in one phase, is found by taking the products of Equations 17 through 20:

$$R_{SA_{n,j}} = \left[\frac{e^{-\sum_{i=1}^{n}\left(\sum_{j=1}^{\text{phase}-1} F_{i,j} + \frac{1}{2}F_{i,j}\right)_{j=\text{abort phase}}} \times \prod_{i=1}^{n}\left(1 + \sum_{j=1}^{\text{phase}-1}\dot{F}_{i,j} + \frac{1}{2}\dot{F}_{i,j}\right)_{j=\text{abort phase}}}{e^{-\left(\sum_{j=1}^{\text{phase}-1} F_{n,j} + \frac{1}{2}F_{n,j}\right)_{j=\text{abort phase}}} \times \left(1 + \sum_{j=1}^{\text{phase}-1}\dot{F}_{n,j} + \frac{1}{2}\dot{F}_{n,j}\right)_{j=\text{abort phase}}}\right] \times \left[e^{-\sum_{j=1}^{\text{phase}-1} F_{n,j}}\left(e^{-\frac{1}{2}F_{n,j}} \times F'_{n,j}\right)_{j=\text{abort phase}}\right]$$

$$\times \left[\frac{e^{-\sum_{i=1}^{n} G_{i,j}}_{j=\text{abort phase}} \times \prod_{i=1}^{n}(1 + \dot{G}_{i,j})}{e^{-G_{n,j}}_{j=\text{abort phase}} \times (1 + \dot{G}_{n,j})}\right] \times \left[e^{-(G_{n,j}-\Delta G_{n,j})}_{j=\text{abort phase}} \times (1 + \dot{G}_{n,j} - 2\Delta G_{n,j})\right]$$

$$\left.\begin{aligned} &= \frac{e^{-\sum_{i=1}^{n}\left(\sum_{j=1}^{\text{phase}-1} F_{i,j} + \frac{1}{2}F_{i,j}\right)} \times \prod_{i=1}^{n}\left(1 + \sum_{j=1}^{\text{phase}-1}\dot{F}_{i,j} + \frac{1}{2}\dot{F}_{i,j}\right)}{\left(1 + \sum_{j=1}^{\text{phase}-1}\dot{F}_{n,j} + \frac{1}{2}\dot{F}_{n,j}\right)} \times F'_{n,j} \\ &\times \frac{e^{-\sum_{i=1}^{n} G_{i,j}} \times \prod_{i=1}^{n}(1 + \dot{G}_{i,j})}{(1 + \dot{G}_{n,j})} \times e^{+\Delta G_{n,j}} \times (1 + \dot{G}_{n,j} - 2\Delta G_{n,j}) \end{aligned}\right\} \quad (21)$$

The probability of safe abort for these cases for all subsystems and all phases is the sum of all $R_{SA_{i,j}}$, $\left(R_{SA} = \sum_{\substack{i=1 \\ j=1}}^{\substack{m \\ n}} R_{SA_{i,j}}\right)$:

$$R_{SA} = \sum_{\substack{i=1\\j=1}}^{\substack{m\\n}} \left[\frac{e^{-\sum_{i=1}^{n}\left(\sum_{j=1}^{phase-1} F_{i,j} + \frac{1}{2} F_{i,j}\right)} \times \prod_{i=1}^{n}\left(1 + \sum_{j=1}^{phase-1} \dot{F}_{i,j} + \frac{1}{2} \dot{F}_{i,j}\right)}{\left(1 + \sum_{j=1}^{phase-1} \dot{F}_{n,j} + \frac{1}{2} \dot{F}_{n,j}\right)} \right.$$

$$\left. \times F'_{n,j} \times \frac{e^{-\sum_{i=1}^{n} G_{i,j}} \times \prod_{i=1}^{n} (1 + \dot{G}_{i,j})}{(1 + \dot{G}_{n,j})} \times e^{+\Delta G_{n,j}} \times (1 + \dot{G}_{n,j} - 2\Delta G_{n,j}) \right] \qquad (22)$$

As in the upper bound case, failure of the SPS in the mission may cause a changed abort mode, and result in changes in the abort logic probabilities for affected subsystems. These are appropriately incorporated into Equations 19, 21, and 22.

The final group of cases—safe abort with more than one failure in the mission in one or more subsystems—utilizes a method of differences. Several probabilities are considered. The sum of these probabilities is equal to the probability of getting to a phase so that, if any one probability is unknown, it can be found by taking the difference between the probability of getting to the phase and the sum of the other probabilities. This fact is used to evaluate cases of multiple failures and, ultimately, crew safety. The probabilities that are summed are:

1. The probability of catastrophic failure;

2. The probability of mission continuation;

3. The probability of an abort with no more than one failure per subsystem.

These are then subtracted from the probability of getting to the phase, and all remaining cases are considered to be attempted aborts.

1. Because the lower bound of crew safety is being computed, calculation of catastrophic failures is performed so as to yield a probability that is on the high side rather than the low side. The overall probability of a catastrophic failure in any phase is a function of the probability of getting to the phase and the probability that a catastrophic failure occurs in the phase. Since a catastrophic failure is the failure of a component that is in series in

both the MC and SA logic diagrams, the probability that a catastrophic failure occurs in a phase is the same for both the upper and lower cases. The variable involved is the difference in the probability of getting to the phase. A higher probability of getting to a phase will result in a greater number of catastrophic failures in the phase. Therefore, when calculating catastrophic failures for the crew safety lower bound, the probability of getting to a phase is obtained from the upper bound MC model. This is found by using Equation 10.

Since the catastrophic failure occurs in one subsystem and at an average time of one-half way through a phase, the other subsystems are satisfactory for this period of time. The probability of these subsystems being good is obtained from Equation 11.

Finally, the probability of a catastrophic failure is found by modifying Equation 12 to include the probability of a catastrophic failure instead of a noncatastrophic one.

Probability of a catastrophic failure equals

$$\underline{e^{-\frac{1}{2}F_{n,j}}\left(F_{n,j} - F'_{n,j}\right)}_{\text{j=abort phase}} \qquad (23)$$

The overall probability of a catastrophic failure for one subsystem (n) in one phase is the product of Equations 10, 11, and 23:

$$P_{CF_{n,j}} = \left(e^{-\sum_{\substack{i=1\\j=1}}^{\substack{\text{phase-1}\\n}} F_{i,j}} \right) \times \left(e_{\text{j=abort phase}}^{-\frac{1}{2}\sum_{i=1}^{n} F_{i,j}} \times e^{+\frac{1}{2}F_{n,j}} \right) \times \left[e^{-\frac{1}{2}F_{n,j}} \left(F_{n,j} - F'_{n,j}\right) \right]$$

$$= e^{-\sum_{\substack{i=1\\j=1}}^{\substack{\text{phase-1}\\n}} F_{i,j}} \times e^{-\frac{1}{2}\sum_{i=1}^{n} F_{i,j}} \times \left(F_{n,j} - F'_{n,j}\right) \qquad (24)$$

The total probability of catastrophic failure of all subsystems in one phase is the sum of the individual subsystem probabilities.

$$P_{CF_j} = \sum_{i=1}^{n} \left[e^{-\sum_{i=1}^{n} \sum_{j=1}^{phase-1} F_{i,j}} \times e^{-\frac{1}{2}\sum_{i=1}^{n} F_{i,j}} \times (F_{i,j} - F'_{i,j}) \right]$$

$$= e^{-\sum_{i=1}^{n} \sum_{j=1}^{phase-1} F_{i,j}} \times e^{-\frac{1}{2}\sum_{i=1}^{n} F_{i,j}} \times \sum_{i=1}^{n} (F_{i,j} - F'_{i,j}) \tag{25}$$

2. Since the crew safety lower bound is found by summing success cases, conservative values of mission continuation utilize lower bound mission success probability calculations. Equation 7 is modified by appropriately changing the limits of the summation.

$$R_{MC_j} = e^{-\sum_{i=1}^{n} \sum_{j=1}^{phase} F_{i,j}} \times \prod_{i=1}^{n} \left(1 + \sum_{j=1}^{phase} \dot{F}_{i,j}\right) \tag{26}$$

3. The probability of an abort in a phase with no more than one failure per subsystem is found by summing the products of Equations 17 and 18 for all subsystems. This is comparable to summing the terms of Equation 21 after deleting those terms concerned with probabilities of successful abort.

$$P_{abort,j} = \sum_{k=1}^{n} \left[\frac{e^{-\sum_{i=1}^{n} \left(\sum_{j=1}^{phase-1} F_{i,j} + \frac{1}{2} F_{i,j} \right)} \times \prod_{i=1}^{n} \left(1 + \sum_{j=1}^{phase-1} \dot{F}_{i,j} + \frac{1}{2}\dot{F}_{i,j}\right)}{\left(1 + \sum_{j=1}^{phase-1} \dot{F}_{k,j} + \frac{1}{2}\dot{F}_{k,j}\right)} \times F'_{k,j} \right] \tag{27}$$

The probability of remaining abort cases per phase is found by subtracting Equations 25, 26, and 27 from the probability of getting to the phase (Equation 7 modified). Remaining abort cases $_j$.

$$= e^{-\sum_{i=1}^{n} \sum_{j=1}^{phase-1} F_{i,j}} \times \prod_{i=1}^{n} \left(1 + \sum_{j=1}^{phase-1} \dot{F}_{i,j}\right) - \left[(25)_j + (26)_j + (27)_j\right] \tag{28}$$

The question arises as to whether some of these remaining cases might be mission continuation cases rather than abort cases because, if they are MC cases, there will be some additional probability of a catastrophic failure in a later phase. However, the probability of catastrophic failure is already based on maximum probability of mission continuation (Equation 25) and includes all possible cases of catastrophic failure. Therefore, for crew safety calculations, it is correct to treat all remaining cases as abort cases.

The probability of achieving a successful abort is, of course, a function of the configuration of the system when the abort is initiated. Since it is not feasible to separate the remaining cases into groups according to which subsystem failure necessitates the abort (because of the complexity resulting from multiple failures), it is necessary to empirically determine an average abort logic applicable to all subsystems which will be conservative, yet not so conservative as to result in an unrealistic number of abort failures.

Two approaches are possible. The first approach is to determine a simple series configuration for each subsystem. This, however, is overly conservative because most subsystems will still have parallel capability.

The second approach, used here, is to assume an average of two failures per subsystem in the mission and appropriately modify each subsystem abort logic. It can be shown that this is very conservative because most subsystems will have incurred less than two failures, and many will have no failures. The Poisson distribution—which applies to conditions in which there are many opportunities for failure but only a small probability of failure at any one opportunity, a typical situation for spacecraft—is utilized. The probabilities of zero and one failure in a subsystem are found, and the appropriate Poisson values are determined. From these, the typical average number of failures per subsystem is well below 1.0 and never above 2.0. Therefore, the probability of successful abort for one subsystem in one phase ($R_{\hat{SA}_{i,j}}$) is found by modifying Equation 20 to take into account two mission failures. This modification is, in itself, conservative because it accounts for noncatastrophic mission failures which have the greatest effect on safe abort probability.

$$R_{\hat{SA}_{i,j}} = \text{Abort prob.}_{i,j} = \underline{e^{-(G_{i,j} - 2\Delta G_{i,j})} \times (1 + \dot{G}_{i,j} - 4\Delta G_{i,j})} \qquad (29)$$

The number of such safe aborts per phase is found by multiplying the number of remaining abort cases in the phase (Equation 28) by the probability of all subsystems being successful, ($\prod_{i=1}^{n}$ Equation 29).

$$R_{\hat{SA}_j} = \left\{ e^{-\sum_{i=1}^{n} \sum_{j=1}^{phase-1} F_{i,j}} \times \prod_{i=1}^{n} \left(1 + \sum_{j=1}^{phase-1} \dot{F}_{i,j} \right) - \left[(25)_j + (26)_j + (27)_j \right] \right\} \times \prod_{i=1}^{n} (29) \tag{30}$$

The total number of such safe aborts is obtained by summing the number for all phases (z) in which an abort is possible.

$$R_{\hat{SA}} = \sum_{j=1}^{z} R_{SA_j} = \sum_{j=1}^{z} (30) \tag{31}$$

In addition to these aborts, the remaining cases which occur during the final mission phases (return, reentry, and post landing) must be considered. The number of these cases is found from Equation 28 in the same manner as for other phases except that Equation 27 is deleted (its value is zero).

The probability of a successful abort, however, cannot be obtained from Equation 29 because there are no separate abort configurations for these phases. To find this probability, the mission success probability for the remaining mission phases, starting half-way through the phase being considered, is determined. This is found from Equations 7 and 26.

$$R_{remain.} = \frac{R_{MS}}{R_{MC_{j-\frac{1}{2}}}} = \frac{e^{-\sum_{i=1}^{n} \sum_{j=1}^{m} F_{i,j}} \times \prod_{i=1}^{n} \left(1 + \sum_{j=1}^{m} \dot{F}_{i,j} \right)}{e^{-\sum_{i=1}^{n} \sum_{j=1}^{phase-\frac{1}{2}} F_{i,j}} \times \prod_{i=1}^{n} \left(1 + \sum_{j=1}^{phase-\frac{1}{2}} \dot{F}_{i,j} \right)}$$

$$= e^{-\sum_{i=1}^{n} \sum_{j=phase-\frac{1}{2}}^{m} F_{i,j}} \times \frac{\prod_{i=1}^{n} \left(1 + \sum_{j=1}^{m} \dot{F}_{i,j} \right)}{\prod_{i=1}^{n} \left(1 + \sum_{j=1}^{phase-\frac{1}{2}} \dot{F}_{i,j} \right)} \tag{32}$$

The number of successful cases is found by multiplying Equation 28 by Equation 32 for each remaining phase.

$$R_{\hat{\hat{SA}}_j} = \left\{ e^{-\sum_{i=1}^{n} \sum_{j=1}^{phase-1} F_{i,j}} \times \prod_{i=1}^{n} \left(1 + \sum_{j=1}^{phase-1} \hat{F}_{i,j}\right) - \left[(25)_j + (26)_j\right] \right\} \times \left[\text{Eq. } (32)\right] \tag{33}$$

The total number of these cases is the sum of the cases for these phases.

$$R_{\hat{\hat{SA}}} = \sum_{j=z+1}^{m} R_{\hat{\hat{SA}}_j} = \sum_{j=z+1}^{m} (33) \tag{34}$$

$R_{\hat{\hat{SA}}_j}$ for the post landing phase, because a successful landing has been accomplished, is considered to be mission success as well as crew safety, and is added into the MS total rather than the SA total. Since the post landing phase is phase m, Equation 32 reduces to approximately unity and the additional number of mission successes is found directly fr 1 Equation 28 applied to phase m.

$$\Delta R_{MS} = \underline{\text{Eq. } (28)_m} \tag{35}$$

Equation 34 is therefore modified by deleting the last phase from the $R_{\hat{\hat{SA}}}$ total:

$$R_{\hat{SA}} = \underline{\sum_{j=z+1}^{m-1} (33)} \tag{36}$$

Finally, the lower bound for crew safety is found by adding the lower bound for mission success (Equations 7 and 35), the number of safe aborts when not more than one failure per subsystem has occurred (Equation 22), and all other cases of safe abort (Equations 31 and 36).

$$\underline{R_{CS_{lower}} = R_{MS_{lower}} + R_{SA_{lower}} + R_{\hat{SA}_{lower}} + R_{\hat{SA}_{lower}}} \tag{37}$$

The overall crew safety reliability is found in the same manner as mission success reliability.

$$\underline{R_{CS} = 1 - \sqrt{(1 - R_{CS})_{upper} \times (1 - R_{CS})_{lower}}} \tag{38}$$

PHASE RELIABILITIES

To determine the reliability of each phase, the upper and lower bounds are determined and suitably combined as shown on page 8 and by Equation 38. The appropriate equations are referenced below although detailed derivations are not presented.

The mission success upper bound for a phase is simply $e^{-\Sigma F_i}$ for that phase as indicated in the discussion on pages 2 and 3. The mission success lower bound is found by dividing the probability of getting through the phase, (Equation 26, j=1 through phase), by the probability of getting to the phase, (Equation 26, j=1 through phase -1).

The crew safety upper bound index is found by subtracting failure cases from unity. The probability of catastrophic failure is obtained directly from Equation 25. The probability of abort failure is found by summing the probabilities of safe aborts in a phase (summation of Equation 15 for all subsystems in the phase) and subtracting this sum from the abort attempts. The attempts are found by summing the products of Equations 10, 11, and 12 for all subsystems in the phase. The crew safety numeric obtained in this manner is an index rather than an exact calculation because the number of failures relates to the particular mission rather than to an independent phase.

The crew safety lower bound is found in the same manner. The probabilities of catastrophic failure, abort failure with zero or one mission failure, and other abort failures are summed, and this sum is subtracted from unity. The probability of catastrophic failure is again obtained directly from Equation 25. The probability of abort failure with zero or one mission failure is the difference between the abort attempts and abort successes—Equation 27 minus the summation of Equation 21 for all subsystems in the phase. Finally, the probability of other abort failures is found by subtracting Equation 30 from Equation 28, or Equation 33 from Equation 28, as applicable.

SUBSYSTEM RELIABILITY

Subsystem reliabilities are found in a manner parallel to that used for phase reliabilities. The mission success upper bound for a subsystem is $e^{-\Sigma F_j}$ for that subsystem. The mission success lower bound is obtained from Equation 6.

The crew safety upper bound index for a subsystem is somewhat more complex. While the probability of catastrophic failure attributed to a subsystem is found simply by summing Equation 24 for all phases, the abort failures charged to the subsystem must be further divided into aborts caused by the subsystem being considered and aborts caused by other subsystems. When the abort is caused by the same subsystem which later causes crew loss, the probability of loss is the product of Equations 10, 11, 12, 13 modified to include half the abort, and (one - Equation 14). When the abort is caused by another subsystem, the probability is the product of Equation 10, Equation 11 modified so that n represents the subsystem causing the abort, Equation 12 also so modified, Equation 13 modified to account for the system which caused the abort and for half the abort time, and (one - Equation 14 modified). And, if the abort is caused by failure of the SPS, suitable changes are made when applicable.

The crew safety lower-bound index is found in a similar manner. The number of abort failures with zero or one failure in the mission is determined by using Equations 17, 18, 19 and (one - Equation 20), appropriately modified. Because there is no accurate method of determining how many of the other abort losses are caused by each subsystem, a simple proportion is used. It is assumed that the percent of these losses per subsystem is the same as the percent of the other abort losses, and the probabilities are computed accordingly.

BLANK PAGE

APPENDIX I. INPUT DATA REQUIREMENTS

The mathematical models which were developed are an optimum compromise between the amount of effort that would be necessary to provide very accurate predictions and the degree of error and approximation that could be accepted without significantly affecting the prediction. Fortunately, the prediction methods presented herein provide satisfactory prediction accuracy without necessitating undue effort on the part of the analysts. The few approximations required from the analysts are such that they will not affect the overall results.

The following inputs, on a phase-by-phase basis, are required for each subsystem:

1. The sum of the failure probabilities of all series elements in MC:

   $\Sigma Q_{k_{MC}}$ (series) where $Q_{k_{MC}} = \lambda_{k_{MC}}$ x t x K factor (environmental) x k factor (contingency)

2. The sum of the failure probabilities of those series elements which are not catastrophic—i.e., series m MC but not series in abort: $\Sigma Q'_{k_{MC}}$

3. The sum of the failure probabilities of the non-series elements in MC (dual redundancy only): $\Sigma\left(\frac{Q_{k\ MC}^{\cdot}}{R_{k\ MC}^{\cdot}}\right)$. If $R_{k\ MC}^{\cdot}$ is greater than 0.999, it can be neglected.

4. The sum of the failure probabilities of all elements considered in MC: $\Sigma Q_{k\ MC}$ (total)

5. The sum of the failure probabilities of the series elements in abort: $\Sigma Q_{k\ SA}$ (series)

6. The sum of the failure probabilities of the non-series elements in abort (dual redundancy only): $\Sigma\left(\frac{Q_{k\ SA}^{\cdot}}{R_{k\ SA}^{\cdot}}\right)$. If $R_{k\ SA}^{\cdot}$ is greater than 0.999, it can be neglected.

7. The sum of the failure probabilities of <u>all</u> elements considered in abort: $\Sigma Q_{k\ SA\ (total)}$

NOTE: In an abort resulting from failure of the SPS, the abort configurations of other subsystems may be affected. When this occurs, sums 5, 6, and 7 will be changed. New sums, 5', 6', and 7', are required in addition to 5, 6, and 7.

8. The sum of the <u>average</u> failure probability of <u>additional</u> elements which become series in abort due to one non-catastrophic series failure in the mission: $\Sigma \Delta Q_{k\ SA\ (series)}$. This is found by determining the average number of additional series elements and multiplying by the average probability of failure in the abort.

APPENDIX II. NAA PROGRAM DESCRIPTION

1. Identification

   a. Program for the Reliability Evaluation of Apollo Mission - REAM - 1M-146 (APF146)

   b. Programmer - F. J. Moskal (7/66)

   c. Space and Information Systems Division (NAA)
      Department 41/200-450

2. Purpose

   REAM is designed to generate an Upper and Lower Reliability Bound for Apollo Mission Success and Crew Safety. These two limits are combined by RMS calculations into an approximately true value. Failure predictions and assessments are calculated on a mission phase, subsystem basis.

3. Restrictions

   a. REAM is written in FORTRAN IV for use in the NAASYS System.

   b. No tapes are required.

   c. Maximum of 25 subsystems and 30 phases are allowed.

4. Method

   a. Upper Bound Case

      Mission Success is determined by:

$$MS = \exp\left\{-\sum_{j=1}^{j=m}\sum_{i=1}^{i=n} F_{j,i}\right\} \quad (1)$$

where $F_{j,i}$ is the probability of failure in mission of subsystem in Phase j

n is the number of subsystems

m is the number of phases

Probability of safe abort from any Phase j caused by failure of any subsystem i is formed by three factors and is given by

$$SA_{m,k} = \underbrace{\left[\exp\left\{-\sum_{j=1}^{j=m-1}\sum_{i=1}^{i=n} F_{j,i}\right\}\right]}_{\text{"A"}} \underbrace{\left[\exp\left\{-\frac{1}{2}\sum_{i=1}^{i=n} F_{m,i}\right\} \cdot F'_{m,k}\right]}_{\text{"B"}}$$

$$\underbrace{\left[\exp\left\{-\sum_{i=1}^{i=n} G_{m,i}\right\} \cdot \exp\left\{-\Delta G_{m,k}\right\}\right]}_{\text{"C"}} \qquad (2)$$

Factor "A" is the "probability of getting to a phase"

Factor "B" is the "probability of non-catastrophic failure"

Factor "C" is the "probability of successful abort"

where $F_{j,i}$ is the probability of failure in mission of subsystem i in Phase j

$F'_{j,i}$ is the probability of non-catastrophic failure in mission of subsystem i in Phase j

$G_{j,i}$ is the probability of failure in abort of subsystem i in Phase j

$\Delta G_{j,i}$ is the additional abort failure probability of subsystem i which failed during mission in Phase j

n is the total number of subsystems

m is the phase in question

k is the subsystem in question

The abort failure probabilities ($G_{j,i}$) of various subsystems are modified by the failure in the mission of the SPS (Service Propulsion Subsystem). This modification occurs in Factor "C" by the replacement of $G_{j,i}$ by a new term $GG_{j,i}$ for each affected subsystem i as shown below

$$\exp \left\{ - \sum_{i=1}^{i=n} \begin{matrix} G_{m,i} \\ GG_{m,i} \end{matrix} \right\}$$

where $GG_{m,i}$ is the modified abort failure probability of subsystem i due to a SPS failure in phase m

The number of catastrophic failures of any subsystem in any phase is given by

$$CF_{m,k} = \underbrace{\left[\exp \left\{ - \sum_{j=1}^{j=m-1} \sum_{i=1}^{i=n} F_{j,i} \right\} \right]}_{\text{"A"}} \underbrace{\left[\exp \left\{ - \frac{1}{2} \sum_{i=1}^{i=n} F_{m,i} \right\} \cdot (F_{m,k} - F'_{m,k}) \right]}_{\text{"D"}} \quad (3)$$

Factor "A" is the "probability of getting to a phase"

Factor "D" is the "probability of a subsystem catastrophically failing half way through a phase

where $F_{j,i}$ is the "probability of failure in mission of subsystem i in Phase j"

$F'_{j,i}$ is the "probability of non-catastrophic failure in mission of subsystem i in Phase j"

n is the total number of subsystems

m is the phase in question

k is the subsystem in question

The number of abort failures caused by the same subsystem that failed in mission is calculated from:

$$AFSS_{m,k} = \underbrace{\left[\exp\left\{-\sum_{j=1}^{j=m-1}\sum_{i=1}^{i=n} F_{j,i}\right\}\right]}_{\text{"A"}} \underbrace{\left[\exp\left\{-\frac{1}{2}\sum_{i=1}^{i=n} F_{m,i}\right\} \cdot F'_{m,k}\right]}_{\text{"B"}} \tag{4a}$$

$$\underbrace{\left[1 - \exp\left\{-(G_{m,k} + \Delta G_{m,k})\right\}\right]}_{\text{"E"}}$$

A special case occurs when the SPS (Service Propulsion Subsystem) fails and is backed up by the LEM (Lunar Excursion Module). The number of abort failures then becomes

$$AFSS_{m,k} = \underbrace{\left[\exp\left\{-\sum_{j=1}^{j=m-1}\sum_{i=1}^{i=n} F_{j,i}\right\}\right]}_{\text{"A"}} \underbrace{\left[\exp\left\{-\frac{1}{2}\sum_{i=1}^{i=n} F_{m,i}\right\}\cdot F'_{m,k}\right]}_{\text{"B"}} \qquad (4b)$$

$$\underbrace{\left[1-\exp\left\{-GG_{m,k}\right\}\right]}_{\text{"E"}}$$

Factor "A" is the probability of getting to a phase

Factor "B" is the probability of non-catastrophic failure

Factor "E" is the probability of abort failure

where $F_{j,i}$ is the probability of failure in mission of subsystem i in Phase j

$F'_{j,i}$ is the probability of non-catastrophic failure in mission of subsystem i in Phase j

$G_{j,i}$ is the probability of failure in abort of subsystem i in Phase j

$\Delta G_{j,i}$ is the additional abort failure probability of subsystem i which failed during mission in Phase j

$GG_{j,i}$	is the modified abort failure probability of subsystem i due to SPS failure in Phase j
n	is the total number of subsystems
m	is the phase in question
k	is the subsystem in question

The number of abort failures caused by a subsystem that did not cause the abort is given by

$$AFDS_{m,k} = \underbrace{\left[\exp\left\{-\sum_{j=1}^{j=m-1}\sum_{i=1}^{i=n} F_{j,i}\right\}\right]}_{\text{"A"}} \left[\underbrace{\left[\sum_{p=1}^{p=n}\left(\exp\left\{-\frac{1}{2}\sum_{i=1}^{i=n} F_{m,i}\right\}\cdot F'_{m,p}\right)\right]}_{\text{"F"}} - \underbrace{\left[\exp\left\{-\frac{1}{2}\sum_{i=1}^{i=n} F_{m,i}\right\}\cdot F'_{m,k}\right]}_{\text{"F Cont."}}\right] \underbrace{\left[1-\exp\left\{-G_{m,k}\right\}\right]}_{\text{"E"}} \qquad (5a)$$

A special case occurs when the SPS fails. The abort failure probabilities of other subsystems are modifed and are reflected in the following relationship:

$$
\begin{aligned}
ASUS_{m,k} = & \underbrace{\left[\exp \left\{ - \sum_{j=1}^{j=m-1} \sum_{i=1}^{i=n} F_{j,i} \right\} \right]}_{\text{"A"}} \left[\left[\left[\left[\sum_{p=1}^{p=n} \left(\exp \left\{ - \frac{1}{2} \sum_{p=1}^{p=n} F_{m,i} \right\} \cdot F'_{m,p} \right) \right] - \right.\right.\right.\right. \\
& \left[\exp \left\{ - \frac{1}{2} \sum_{i=1}^{i=n} F_{m,i} \right\} \cdot F'_{m,k} \right] - \left[\exp \left\{ - \frac{1}{2} \sum_{i=1}^{i=n} F_{m,i} \right\} \cdot F'_{m,r} \right] \Bigg] \qquad (5b) \\
& \left[1 - \exp \left\{ - G_{m,k} \right\} \right] \Bigg] + \left[\exp \left\{ - \frac{1}{2} \sum_{i=1}^{i=n} F_{m,i} \right\} \cdot F'_{m,r} \right] \left[1 - \exp \left\{ - GG_{m,k} \right\} \right] \Bigg]
\end{aligned}
$$

Factor "A" is the probability of getting to a phase

Factor "F" is the probability of no failures of all other subsystems

Factor "E" is the probability of abort failure

Note that some factors in the special case are not identified. The probability of no failures of all other subsystems and the probability of abort failure are combined into one term.

where $F_{j,i}$ is the probability of failure in mission of subsystem i in Phase j

$F'_{j,i}$ is the probability of non-catastrophic failure in mission of subsystem i in Phase j

$G_{j,i}$ is the probability of failure in abort of subsystem i in Phase j

$\Delta G_{j,i}$ is the additional abort failure probability of subsystem i which failed in mission in Phase j

$GG_{j,i}$ is the additional abort failure probability of subsystem i due to SPS failure in Phase j

n is the total number of subsystems

m is the phase in question

k is the subsystem in question

r is the SPS subsystem

b. Lower Bound.

The mission continuation probability is given by

$$MCP_{m,n} = \left[\exp - \left\{ - \sum_{j=1}^{j=m} F_{j,n} \right\} \right] \left[1 + \sum_{j=1}^{j=m} \dot{F}_{j,n} \right] \qquad (6)$$

where $F_{j,i}$ is the probability of failure in mission for all elements of subsystem i in Phase j

$\dot{F}_{j,i}$ is the probability of failure in mission for non-series elements of subsystem i in Phase j

m is the phase in question

n is the subsystem in question

The probability of getting through a phase from phase one is given by:

$$PGT_m = \prod_{p=1}^{p=n} \left[\left[\exp \left\{ - \sum_{j=1}^{j=m} F_{j,p} \right\} \right] \left[1 + \sum_{j=1}^{j=m} \dot{F}_{j,p} \right] \right] \tag{7}$$

where $F_{j,i}$ is the probability of failure in mission for all elements of subsystem i in Phase j

$\dot{F}_{j,i}$ is the probability of failure in mission for non-series elements of subsystem i in Phase j

m is the phase in question

n is the total lnumber of subsystems

The reliability of a phase m is given by the quotient (from Equation 7)

$$ROPH_m = \frac{PGT_m}{PGT_{m-1}} \tag{8}$$

Note that $ROPH_1 = PGT_1$

The probability of getting half way through a phase m, from phase 1 is obtained by

$$HAFWAY_m = \prod_{p=1}^{p=n} \left[\left[\exp \left\{ - \left(\left(\sum_{j=1}^{j=m-1} F_{j,p} \right) + \frac{1}{2} F_{m,p} \right) \right\} \right] \left[1 + \left(\sum_{j=1}^{j=m-1} \dot{F}_{j,p} \right) + \frac{1}{2} \dot{F}_{m,p} \right] \right] \tag{9}$$

where $F_{j,i}$ is the probability of failure in mission for all elements of subsystem i in phase j

$\dot{F}_{j,i}$ is the probability of failure in mission for non-series elements of subsystem i in phase j

m is the phase in question

n is the total number of subsystems

The number of aborts caused by subsystem i in phase j is given by

$$ABTN_{m,n} = \frac{\left[\prod_{p=1}^{p=m} \left[\left[\exp \left\{ - \left(\left(\sum_{j=1}^{j=m-1} F_{j,p} \right) + \frac{1}{2} F_{m,p} \right) \right\} \right] \left[1 + \left(\sum_{j=1}^{j=m-1} \dot{F}_{j,p} \right) + \frac{1}{2} \dot{F}_{m,p} \right] \right] \cdot F'_{m,n} \right]}{\left[1 + \left(\sum_{j=1}^{j=m-1} \dot{F}_{j,n} \right) + \frac{1}{2} \dot{F}_{m,n} \right]} \tag{10}$$

where $F_{j,i}$ is the probability of failure in mission for all elements of subsystem i in phase j

$\dot{F}_{j,i}$ is the probability of failure in mission for non-series elements of subsystem i in phase j

$F'_{j,i}$ is the probability of non-catastrophic failure in mission of subsystem i in phase j

m is the phase in question

n is the subsystem in question

The probability of safe abort is determined from

$$PSA_{m,k} = \frac{\left[\exp\left\{-\sum_{i=1}^{i=n} G_{m,i}\right\}\right]\left[\prod_{i=1}^{i=n}\left(1 + \dot{G}_{m,i}\right)\right]\left[\exp\left\{\Delta G_{m,k}\right\}\right]\left[1 + \dot{G}_{m,k} - 2\Delta G_{m,k}\right]}{\left(1 + \dot{G}_{m,k}\right)} \qquad (11a)$$

A special case occurs when the SPS fails. The abort failure probabilities of some other subsystems are modified. This modification is shown in the following equation where GG and $\dot{G}\dot{G}$ terms replaces G and $\dot{G}$ terms if applicable.

$$PSA_{m,k} = \frac{\left[\exp\left\{-\sum_{i=1}^{i=n} \begin{matrix} G_{m,i} \\ GG_{m,i} \end{matrix}\right\}\right]\left[\prod_{i=1}^{i=n}\left(1 + \begin{matrix} \dot{G}_{m,i} \\ \dot{G}\dot{G}_{m,i} \end{matrix}\right)\right]\left[\exp\left\{\Delta G_{m,k}\right\}\right]\left[1 + \dot{G}_{m,k} - 2\Delta G_{m,k}\right]}{\left(1 + \dot{G}_{m,k}\right)} \qquad (11b)$$

where $G_{j,i}$ is the probability of failure in abort for all elements of subsystem i in phase j

$\dot{G}_{j,i}$ is the probability of failure in abort for all non-series elements of subsystem i in phase j

$\Delta G_{j,i}$ is the additional abort failure probability of subsystem i which failed during mission in phase j

$GG_{j,i}$ and $\dot{G}\dot{G}_{j,i}$ are the modified abort failure probabilities of subsystem i due to SPS failure in phase j

n is the total number of subsystems

	m	is the phase in question
	k	is the subsystem in question

The number of safe aborts per subsystem in any phase is given by the product of the two values just calculated

$$NSA_{m,k} = \left[ABTN_{m,k}\right] \quad \left[PSA_{m,k}\right] \tag{12}$$

where	m	is the phase in question
	k	is the subsystem in question

The contribution of multiple failures of all other subsystems to crew fatality in the abort mode is given by

$$MFAM_{m,k} = \frac{\left[\exp\left\{ -\sum_{i=1}^{i=n} G_{m,i}\right\}\right]\left[\prod_{i=1}^{i=n}\left(1 + \mathring{G}_{m,i}\right)\right]}{\left[\exp\left\{- G_{m,k}\right\}\right]\left[\left(1 + \mathring{G}_{m,k}\right)\right]} \tag{13}$$

where	$G_{j,i}$	is the probability of failure in abort for all elements of subsystem i in phase j
	$\mathring{G}_{j,i}$	is the probability of failure in abort for all non-series elements of subsystem i in phase j
	n	is the total number of subsystems
	m	is the phase in question
	k	is the subsystem in question

The number of abort failures caused by the same subsystem that failed in mission is determined from

$$AFSS_{m,k} = HAFWAY_m \underbrace{\left[\frac{F'_{m,k}}{1 + \left(\sum_{j=1}^{j=m-1} \dot{F}_{j,k} \right) + \frac{1}{2} \dot{F}_{m,k}} \right]}_{\text{"G"}} \underbrace{\left[1 - \frac{1 - MFAM_{m,k}}{2} \right]}_{\text{"H"}} \qquad (14a)$$

$$\left[1 - \exp \left\{ \left(- G_{m,k} - \Delta G_{m,k} \right) \right\} \right] \left[1 + \dot{G}_{m,k} - 2\Delta G_{m,k} \right]$$

A special case occurs when the SPS fails the abort failure probabilities of some other subsystems are modifed. This modification is illustrated in the following equation

$$AFSS_{m,k} = HAFWAY_m \underbrace{\left[\frac{F'_{m,k}}{1 + \left(\sum_{j=1}^{j=m-1} \dot{F}_{j,k} \right) + \frac{1}{2} \dot{F}_{m,k}} \right]}_{\text{"G"}} \underbrace{\left[1 - \frac{1 - MFAM_{m,k}}{2} \right]}_{\text{"H"}} \qquad (14b)$$

$$\left[1 - \exp \left\{ - GG_{m,k} \right\} \right] \left[1 + \dot{GG}_{m,k} \right]$$

Factor "G" is the probability of getting halfway through a phase (Equation 9)

Factor "H" is the probability that one half the multiple failures will be fatal to the crew (from Equation 13)

where $G_{j,i}$ is the probability of failure in abort for all elements of subsystem i in phase j

$\dot{G}_{j,i}$ is the probability of failure in abort for all non-series elements of subsystem i in phase j

$\Delta G_{j,i}$ is the additional abort failure probability of subsystem i which failed during mission in phase j

$\dot{F}_{j,i}$ is the probability of failure in mission for non-series elements of subsystem i in phase j

$F'_{j,i}$ is the probability of non-catastrophic failure in mission of subsystem i in phase j

$GG_{j,i}$ and $\dot{G}\dot{G}_{j,i}$ are the modified abort failure probabilities of subsystem i due to a SPS failure in phase j

The number of abort failures caused by a subsystem that did not cause the abort is given by

$$\mathrm{AFDS}_{m,k} = \underset{\text{"G"}}{\mathrm{HAFWAY}_m}\left[\left[\sum_{\ell=1}^{\ell=m}\left(\frac{F'_{m,\ell}}{1 + \sum\limits_{j=1}^{j=m-1}\dot{F}_{j,\ell} + \frac{1}{2}\dot{F}_{m,\ell}}\right)\right] - \left[\frac{F'_{m,\ell}}{1 + \sum\limits_{j=1}^{j=m-1}\dot{F}_{j,m} + \frac{1}{2}\dot{F}_{m,k}}\right]\right] \tag{15a}$$

$$\underbrace{\left[1 - \frac{1 - \mathrm{MFAM}_{m,k}}{2}\right]}_{\text{"H"}}\left[1 - \exp\left\{-G_{m,k}\right\}\right]\left[1 + \dot{G}_{m,k}\right]$$

A special case occurs when the SPS fails. The abort failure probabilities of some other subsystems are modified as shown below.

$$\mathrm{AFDS}_{m,k} = \underset{\text{"G"}}{\mathrm{HAFWAY}_m}\underbrace{\left[1 - \frac{1 - \mathrm{MFAM}_{m,k}}{2}\right]}_{\text{"H"}}\left[\left[\left[\sum_{\ell=1}^{\ell=m}\left(\frac{F'_{m,\ell}}{1 + \sum\limits_{j=1}^{j=m-1}\dot{F}_{j,\ell} + \frac{1}{2}\dot{F}_{m,\ell}}\right)\right] -\right.\right.$$

$$\left.\left[\frac{F'_{m,k}}{1 + \sum\limits_{j=1}^{j=m-1}\dot{F}_{j,k} + \frac{1}{2}\dot{F}_{m,k}}\right] - \left[\frac{F'_{m,r}}{1 + \sum\limits_{j=1}^{j=m-1}\dot{F}_{j,r} + \frac{1}{2}\dot{F}_{m,r}}\right]\right]\left[1 - \exp\left\{-G_{m,k}\right\}\right]\left[1 + \dot{G}_{m,k}\right] +$$

$$\left.\left[\frac{F'_{m,r}}{1 + \sum\limits_{j=1}^{j=m-1}\dot{F}_{j,r} + \frac{1}{2}\dot{F}_{m,r}}\right]\left[1 - \exp\left\{-GG_{m,k}\right\}\right]\left[1 + \dot{G}\dot{G}_{m,k}\right]\right] \tag{15b}$$

Factor "G" is the probability of getting halfway through a phase (Equation 9)

Factor "H" is the probability that one half of the multiple failures will be fatal to the crew (from Equation 13)

where $G_{j,i}$ is the probability of failure in abort for all elements of subsystem i in phase j

$\dot{G}_{j,i}$ is the probability of failure in abort for all non-series elements of subsystem i in phase j

$\Delta G_{j,i}$ is the additional abort failure probability of subsystem i which failed during mission in phase j

$\dot{F}_{j,i}$ is the probability of failure in mission for non-series elements of subsystem i in phase j

$F'_{j,i}$ is the probability of non-catastrophic failure in mission of subsystem i in phase j

$GG_{j,i}$ and $\dot{G}\dot{G}_{j,i}$ are the modified abort failure probabilities of subsystem i due to a SPS failure in phase j

The approximate true value of the failure probability is obtained by taking the square root of the product of the upper and lower values of the probability of failure

$$RMS = 1 - \sqrt{\underset{(Eq.\ 1)}{(1 - MS)}\ \underset{(Eq.\ 6)}{(1 - MCP)}}$$

5. <u>Input Data</u>

Card No. 1 Comments

Program data description from this card is printed at the tops of each output page. Comments, program titles, test block number, date, etc. may occupy columns 1 - 80. Centering the comment on the card will center the comment on the output page.

Card No. 2 Data Size

c.c.	
11 - 12	Number of Phases (right adjusted) 30 maximum
23 - 24	Number of Subsystems (right adjusted) 25 maximum

Card Group No. 3 Subsystem Names

Subsystem name abbreviations are written one on each card in columns 1 - 12. There should be a subsystem name card for each subsystem and should be queued in the same order as the input data.

Card No. 4 Control

c.c.	
1 - 80	Must contain all 9's

This card separates the subsystem name cards from the upper bound input data cards.

Card Group No. 5 Upper Bound Data

c.c.	
1 - 12	Mission Failure Probability
13 - 24	Abort Failure Probability
25 - 30	Mission Failure Probability (non-catastrophic)

31 - 36	Additional Abort Failure Probability
37 - 48	Modified Abort Failure Probability (SPS Failure)
73	SPS Backup Indicator
	1 for RCS
	2 for LEM
74 - 76	Phase Number (right adjusted)
77 - 80	Subsystem Number (right adjusted)

There should be a card for each subsystem in each phase. The cards may be in any order.

Card No. 6 Control

c.c.	
1 - 80	Must contain all 9's

This card separates the upper bound data from the lower bound data.

Card Group No. 7 Lower Bound Data

c.c.	
1 - 8	Mission Failure Probability All Elements
9 - 16	Mission Failure Probability All Non-Series Elements
17 - 24	Abort Failure Probability All Elements
25 - 32	Abort Failure Probability All Non-Series Elements
33 - 40	Mission Failure Probability Non-Catastrophic
41 - 48	Modified Abort Failure Probability
49 - 56	Modified Abort Failure Probability
57 - 64	Additional Abort Failure Probability
73	SPS Backup Indicator
	1 for RCS
	2 for LEM

74 - 76	Phase Number (right adjusted)
77 - 80	Phase Number (right adjusted)

There should be a card for each subsystem in each phase. The card may be in any order.

Card No. 8 Control

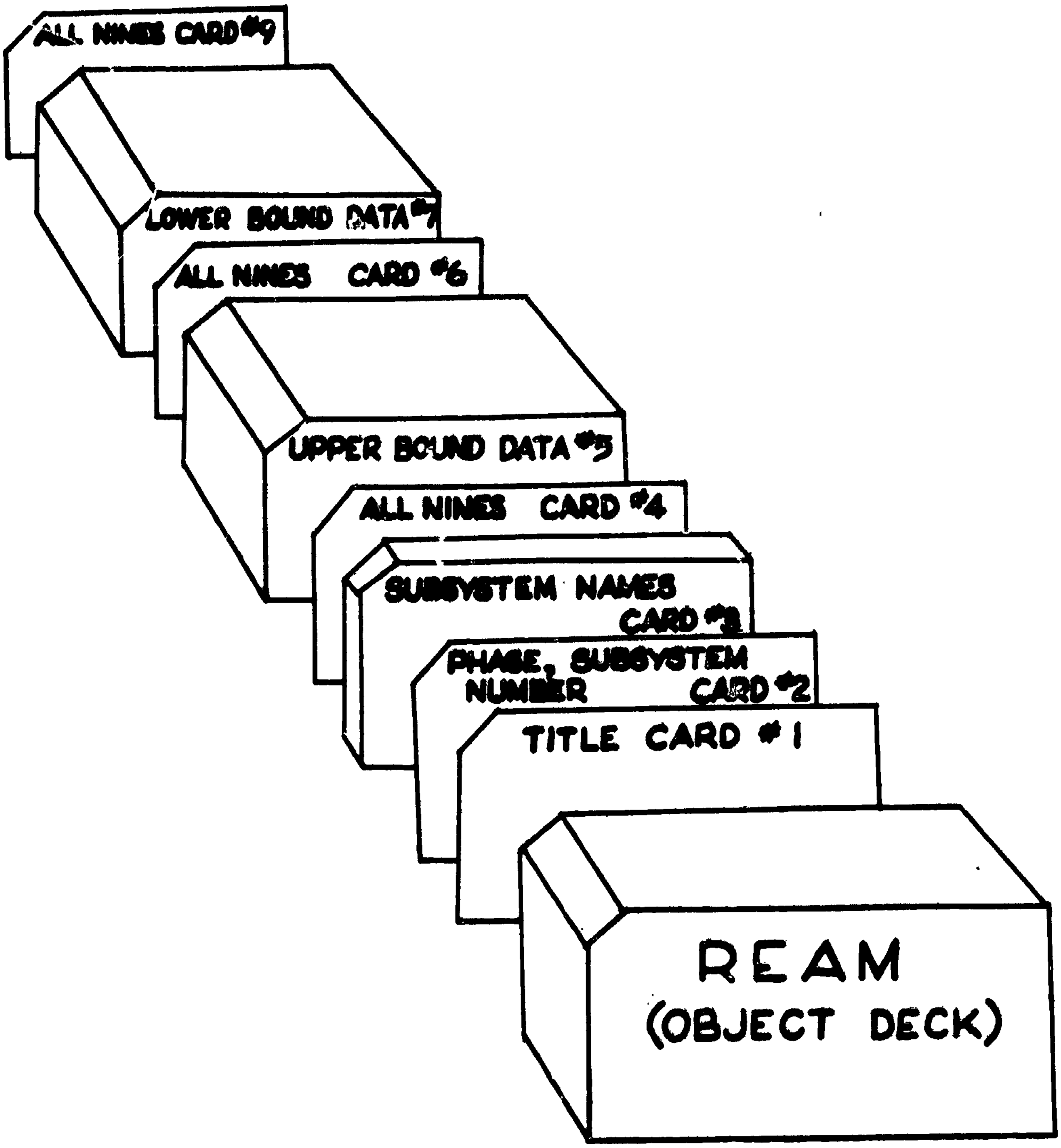
This card terminates the data read.

6. Appendices

Appendix I - Deck Setup

Appendix II - Sample Data

Appendix III - Samplet Output


ALL NINES CARD #9
LOWER BOUND DATA #7
ALL NINES CARD #6
UPPER BOUND DATA #5
ALL NINES CARD #4
SUBSYSTEM NAMES CARD #3
PHASE, SUBSYSTEM NUMBER CARD #2
TITLE CARD #1
REAM
(OBJECT DECK)

FORTRAN WORK SHI

DECK NO. ______ PROGRAMMER ______ DA

FOR PROGRAM NO. ______ TITLE ______

```
         10        20        30        40
                    MISSIØN EVALUATIØN  SAMPLE D
            2            3
PS
M /RCS
M/ RCS
<
00 0600     .00 0523     .000 580     .00386
00 0259     .00 0639     .000 259     .01002
00 0093     .00 0076     .000 052     .00085
00 0060     .00 0052     .000 058     .00038
00 0025     .00 0063     .000 025     .00100
00 0009     .00 0007     .000 005     .00008
<
00 0690  .00 0090  .0 0524  .005 296  .000 580
00 1187  .00 0928  .0 02757  .002 278  .000 259  .04 2956
00 0318  .00 0225  .0 00412  .000 336  .000 052
00 0069  .00 0009  .0 00581  .000 529  .000 058
00 0118  .00 0092  .0 00221  .000 227  .000 025  .000 692
00 0031  .00 0022  .0 00041  .000 033  .000 005
0 <
```

Form 114-D-20

A 1

WORK SHEET

DATE ____ PAGE ____ OF ____ JOB NO. ____

BY DEPT. ____ GROUP ____

40	50	60	70	IDENTIFICATION 73–80
SAMPLE DATA				
				9
0386				1 1 1
1002	.009008			1 2
0085				1 3
0038				1 2 1
0100	.000900			2 2
0008				2 3
				9
0		.003886		1 1
9 .042956	.006925	.010002		2 1 2
2				1 3
8		.000038		2 1
5 .000692	.000100			2 2 2
5				2 3
				9

APPENDIX III. MISSION EVALUATION SAMPLE DATA

MISSION EVALUATION SAMPLE DATA
INPUT DATA JPPER BOUND CASE
PHASE 1

SUBSYSTEM	MISSION FAILURE PROBABILITY	ABORT FAILURE PROBABILITY	MISSION FAILURE PROBABILITY NON-CATASTROPHIC	ADDITIONAL ABORT FAILURE PROBABILITY	MODIFIED ABORT FAILURE PROBABILITY
SPS	0.0006CC	0.000523	0.JC0580	0.000386	0.J00000
SM/RCS	0.000259	0.000639	0.JC0259	0.001002	0.009008
CM/RCS	0.000G93	0.000076	0.JC0052	0.000085	G.000000

MISSION EVALUATION SAMPLE DATA
INPUT DATA UPPER BOUND CASE
PHASE 2

SUBSYSTEM	MISSION FAILURE PROBABILITY	ABORT FAILURE PROBABILITY	MISSION FAILURE PROBABILITY NON-CATASTROPHIC	ADDITIONAL ABORT FAILURE PROBABILITY	MODIFIED ABORT FAILURE PROBABILITY
SPS	0.000060	0.000052	0.000058	0.000038	0.000000
SM/RCS	0.000025	0.000063	0.000025	0.000100	0.000900
CM/RCS	0.000009	0.000007	0.000005	0.000008	0.000000

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA UPPER BOUND CASE
PHASE 1

SUBSYSTEM	SAFE ABORT PROBABILITY		CATASTROPHIC FAILURE PROBABILITIES			
			MISSION		ABORT	
	TOTAL	PARTIAL	TOTAL	PARTIAL	SAME SUBSYSTEM	OTHER SUBSYSTEM
SPS	0.000574	0.000580	0.000020	0.000020	0.000001	0.000000
SM/RCS	0.000258	0.000259	0.000000	0.000000	0.000000	0.000005
CM/RCS	0.000052	0.000052	0.000041	0.000041	0.000000	0.000000

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA JPPER BOUND CASE
PHASE 2

SUBSYSTEM	SAFE ABORT PROBABILITY		CATASTROPHIC FAILURE PROBABILITIES			
			MISSION		ABORT	
	TOTAL	PARTIAL	TOTAL	PARTIAL	SAME SUBSYSTEM	OTHER SUBSYSTEM
SPS	0.000058	0.000058	0.000002	0.000002	0.000000	0.000000
SM/RCS	0.000025	0.000025	0.000000	0.000000	0.000000	0.000000
CM/RCS	0.000005	0.000005	0.000004	0.000004	0.000000	0.000000

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA UPPER BOUND CASE

PHASE	RELIABILITY OF PHASE	RELIABILITY TO PHASE	CATASTROPHIC FAILURE PROBABILITIES			SAFE ABORT PROBABILITY	CREW SAFETY INDEX
			MISSION	MISSION PARTIAL	ABORT		
1	0.999948	1.000000	0.000061	0.000061	0.000006	0.000884	0.999933
2	0.999906	0.999048	0.000006	0.000006	0.000000	0.000088	0.999994

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA JPPER BOUND CASE

SUBSYSTEM	RELIABILITY OF SUBSYSTEM	CATASTROPHIC FAILURE PROBABILITIES MISSION	ABORT SAME SUBSYSTEM	ABORT OTHER SUBSYSTEM	CREW FATALITY OF SUBSYSTEM	CREW SAFETY INDEX
SPS	0.999340	0.000022	0.000001	0.000000	0.000023	0.999977
SM/RCS	0.999716	0.000000	0.000000	0.000005	0.000006	0.999994
CM/RCS	0.999898	0.000045	0.000000	0.000000	0.000045	0.999955

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA JPPER BOUND CASE

RELIABILITY OF MISSION	CATASTROPHIC FAILURE PROBABILITIES			CREW FATALITY OF MISSION	SAFE ABORT PROBABILITY
	MISSION	ABORT SAME SUBSYSTEM	ABORT OTHER SUBSYSTEM		
0.998955	0.000067	0.000001	0.000006	0.000073	0.000972

MISSION EVALUATION SAMPLE DATA
INPUT DATA LOWER BOUND CASE
PHASE 1

SUBSYSTEM	MISSION FAILURE PROBABILITY		ABORT FAILURE PROBABILITY		MISSION FAILURE PROBABILITY NON	MODIFIED ABORT FAILURE		ADDITIONAL ABORT FAILURE
	ALL ELEMENTS	NON SERIES ELEMENTS	ALL ELEMENTS	NON SERIES ELEMENTS	CATASTROPHIC	PROBABILITIES		PROBABILITY
SPS	0.000690	0.000090	0.005524	0.005296	0.000580	0.000000	0.000000	0.000386
SM/RCS	0.001187	0.000928	0.032757	0.002278	0.000259	0.042956	0.006925	0.001002
CM/RCS	0.000318	0.000225	0.000412	0.000336	0.000052	0.000000	0.000000	0.000085

MISSION EVALUATION SAMPLE DATA
INPUT DATA LOWER BOUND CASE
PHASE 2

SUBSYSTEM	MISSION FAILURE PROBABILITY		ABORT FAILURE PROBABILITY		MISSION FAILURE PROBABILITY NON	MODIFIED ABORT FAILURE PROBABILITIES		ADDITIONAL ABORT FAILURE PROBABILITY
	ALL ELEMENTS	NON SERIES ELEMENTS	ALL ELEMENTS	NON SERIES ELEMENTS	CATASTROPHIC			
SPS	0.000069	0.000009	0.000581	0.000529	0.000058	0.000000	0.000000	0.000038
SM/RCS	0.000118	0.000092	0.000221	0.000227	0.000025	0.004295	0.000692	0.000100
CM/RCS	0.000031	0.000022	0.000041	0.000033	C.C00005	0.000000	0.000000	0.000008

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA LOWER BOUND CASE
PHASE 1

SUBSYSTEM	RELIABILITY OF SUBSYSTEM	PROBABILITY OF AN ABORT	ABORT CALCULATIONS RELIABILITY OF AN ABORT	SAFE ABORT PROBABILITY
SPS	0.999400	0.000580	0.963912	0.000559
SM/RCS	0.999741	0.000259	0.998203	0.000258
CM/RCS	0.999907	0.000052	0.999116	0.000052

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA LOWER BOUND CASE
PHASE 2

SUBSYSTEM	RELIABILITY OF SUBSYSTEM	ABORT CALCULATIONS PROBABILITY OF AN ABORT	RELIABILITY OF AN ABORT	SAFE ABORT PROBABILITY
SPS	0.999340	0.C00058	0.996305	0.000058
SM/RCS	0.999715	0.C00025	0.999846	0.000025
CM/RCS	0.999898	0.000005	0.999938	0.000005

MISSION EVALUATION SAMPLE DATA

OUTPUT DATA LOWER BOUND CASE

PHASE	RELIABILITY THRU PHASE	RELIABILITY OF PHASE	RELIABILITY 1/2 THRU PHASE	ONE FAILURE PROBABILITY ABORT	ONE FAILURE PROBABILITY SAFE ABORT	OTHER CASES PROBABILITY ABORT	OTHER CASES PROBABILITY SUCCESS	OTHER CASES PROBABILITY SAFE ABORT
1	0.999048	0.999048	0.999524	0.000890	0.000869	0.000001	0.999429	0.000001
2	0.998953	0.999905	0.999030	0.000088	0.000088	0.000001	1.000000	0.000001

MISSION EVALUATION SAMPLE DATA

OUTPUT DATA LOWER BOUND CASE

PHASE	RELIABILITY OF PHASE	CATASTROPHIC FAILURE PROBABILITIES ONE FAILURE ABORTS	OTHER ABORTS	MISSION	TOTAL	CREW SAFETY INDEX
1	0.999048	0.000021	0.000000	0.000061	0.000082	0.999918
2	0.999905	0.000000	0.000000	0.000006	0.000006	0.999994

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA LOWER BOUND CASE

SUBSYSTEM	RELIABILITY OF SUBSYSTEM	CATASTROPHIC FAILURE PROBABILITIES ABORT ONE FAILURE	OTHERS	MISSION	TOTAL	CREW SAFETY INDEX
SPS	0.999340	0.000000	0.000000	0.000022	0.000022	0.999978
SM/RCS	0.999715	0.000021	0.000000	0.000000	0.000021	0.999979
CM/RCS	0.999898	0.000000	0.000000	0.000045	0.000045	0.999955

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA LOWER BOUND CASE

RELIABILITY OF MISSION	SAFE ABORT PROBABILITIES ONE FAILURE	OTHERS	TOTAL	CREW FATALITY OF MISSION
0.998954	0.000957	0.000001	0.000957	0.000089

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA RMS CALCULATIONS

PHASE	RELIABILITY OF PHASE			CREW SAFETY INDEX OF PHASE		
	LOWER BOUND	UPPER BOUND	RMS VALUE	LOWER BOUND	UPPER BOUND	RMS VALUE
1	0.999048	0.999048	0.999048	0.999918	0.999933	0.999925
2	0.999905	0.999906	0.999905	0.999994	0.999994	0.999994

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA RMS CALCULATIONS

SUBSYSTEM	RELIABILITY OF SUBSYSTEM			CREW SAFETY INDEX OF SUBSYSTEM		
	LOWER BOUND	UPPER BOUND	RMS VALUE	LOWER BOUND	UPPER BOUND	RMS VALUE
SPS	0.999340	0.999340	0.999340	0.999978	0.999977	0.999977
SM/RCS	0.999715	0.999716	0.999715	0.999979	0.999994	0.999989
CM/RCS	0.999898	0.999898	0.999898	0.999955	0.999955	0.999955

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA RMS CALCULATIONS

RELIABILITY OF MISSION			CREW SAFETY OF MISSION		
LOWER BOUND	UPPER BOUND	RMS VALUE	LOWER BOUND	UPPER BOUND	RMS VALUE
0.998954	0.998955	0.998954	0.999911	0.999927	0.999919

MISSION EVALUATION SAMPLE DATA
OUTPUT DATA RMS CALCULATIONS

RELIABILITY OF MISSION			CREW SAFETY OF MISSION		
LOWER BOUND	UPPER BOUND	RMS VALUE	LOWER BOUND	UPPER BOUND	RMS VALUE
0.998954	0.998955	0.998954	0.999911	0.999927	0.999919